Installation Innovation: What's Next? **Insight by Lucian Niemeyer**

Since the release of the National Defense Strategy (NDS) in February 2018, our priorities have been revised to ensure that our installations, the platforms from which we generate and project power from a range of mission capabilities, are resilient to an ever-growing range of threats and ready for new generations of weapons systems. As a result, **innovations in future installation planning and the determination of military value must incorporate the needs of new technologies and the risk assessments of resilience for the critical mission capabilities.**

The first question for the innovation of our installations is what new technologies should we be planning for? While difficult to predict the future of warfare, current military research and development efforts portend installation support for the manning of multi-mission command centers controlling a myriad of space, cyber, robotic, and unmanned systems deploying kinetic effects from the air, sea, and land. Bases will be part of a comprehensive network of command elements. As a result, resilient and robust communications across global networks will be needed to sustain critical connectivity with assured electricity and a growing demand for secure and backhaul, bandwidth and spectrum. Critical assets and forces across all spectrums (air, land, sea, space, spectrum, cyberspace) will need to be protected (include thermal masking and signal jamming), dispersed, and mobile. All types of data networks will need redundancy and increased security to provide mission assurance. Those same networks may also be the delivery method for adversaries wanting to use a cyberattack to disrupt the mission of, or even physically destroy/disable a facility through the exploitation of control systems. Therefore future installations will need to be as secure as they are smart. Fossil fueled engines and combustion propellants will eventually be displaced by electromagnetic effects driving increased, distributed power generation requirements. Future installations will deploy equipment and supplies with rotary wing unmanned logistics systems.

As future forces will value distance and speed of systems, future ranges will need more space to train the next generation of hypersonic weapons, high speed delivery systems, and other long range munitions. Future ranges will support the test and training of unmanned/autonomous vehicle with electromagnetic or directed energy weapons. Range threat emitter packages will be need to evolve with the rapidly changing threats. Ranges will also need to support tactical units using nanotechnologies and new weapons in highly dense, urban terrains.

As for the installation resilience to support these technologies, The NDS outlines two imperatives:

1) **The homeland is no longer a sanctuary.** America is a target from enemies seeking to attack our citizens, our infrastructure, and to use political and information subversion. During conflict, we must anticipate attacks against our military bases at home with effects carrying beyond the fencelines to our national infrastructure.

2) **Today, every domain is contested.** Therefore the threats challenging installation resilience are multi-faceted, extending across domains.

As we look to innovation in the bases of the future, we define installation resilience as the ability of platforms around the world to accomplish their missions despite deliberate actions by adversaries or natural

events to deny, disrupt, exploit, or destroy the missions on our bases. We continually assess mission resiliency in an increasingly complex security environment defined by rapid technological challenges. Many vulnerabilities we must address today did not exist a decade or even five years ago. While concerns of installation resilience have, in the past, focused on natural events, the growth and range of adversary threats today represent more complex challenges. We are tackling these challenges holistically across six broad categories: contingency, energy and water, data, control systems cybersecurity, physical security, and environmental resilience. We mitigate these risks amidst competing priorities through a comprehensive mission assurance evaluation for each critical facility to enhance readiness and lethality in defense of America's interests anytime, anywhere.

The Department's ability to protect our Nation's interests and those of our allies around the globe is dependent on the resilience of our main operating bases - the survivability of expeditionary bases and cooperative security locations are equally important. Significant long-term risk to installation resilience from the exertion of political will can limit access to military bases and on ranges. While this concern is particularly acute overseas as adversaries employ various forms of coercion, activism, or economic levers to influence host nations or allies to limit cooperative security and access to ports, facilities, airfields and other infrastructure, we are seeing similar situations domestically with special interests influencing our defense communities and States. We must continue to work collaboratively with defense communities, and our host nations to counter initiatives to reduce or eliminate our presence or operations.

Our adversaries also have the ability to strike our large force concentrations anywhere in the world. In response, we must prioritize authorities and resources needed to balance centralized, soft infrastructure with smaller, dispersed, resilient basing. We have initiatives underway to develop new locations within the Europe and the Indo-Pacific for the placement of forces and will need to quickly construct facilities to support rapid force dispersal and protection. We must also innovatively address resilient and agile logistics to include access to fuel around the world and on future battlefields. We are prioritizing installation requirements for prepositioned forward fuel, stocks, and munitions to ensure sustainment in a contested environment.

In the energy domain, revolutionary technological changes using artificial intelligence, robotics, autonomous systems, advanced telecommunications and additive manufacturing have ONE common critical enabler – electricity. In the near future, we will also NEED MORE electricity to power new generations of vehicles, sensors, cyber forces, and directed energy weapons. Our adversaries are already seeking to counter these superior technologies asymmetrically, with cheap methods to deny, disrupt or attack our energy supply and distribution systems. Our infrastructure is being tested and probed today; cyber threats to our electrical grid are real and growing. Energy resilience depends on the flexibility to counter these threats by using all fuel sources (from fossil fuels to micro nuclear reactors and renewables) effectively and efficiently to meet critical mission priorities. We have reached out to local utilities and the private sector to collaborate on initiatives to improve energy management while reducing vulnerabilities outside the fence lines of our bases.

We are also collaborating with industry and defense communities on the national development of small cell technology and a Fifth Generation (5G) network. Our goal is to reduce the threat of foreign cyberattacks or disruption to this new infrastructure. We know the quality and speed of the decisions, enabled by software and data through wireless networks will drive both an economic and military edge for our country. As such, these networks must be resilient and secure. A whole new generation of weapons systems, unmanned systems,

autonomous vehicles, robotics and artificial intelligence will rely on, and are effected by, how fast we can transmit data. .The military value for the "base of the future" will depend on the availability, resilience, and security of 5G infrastructure. As such, States and local communities having an economic stake in national defense must take an active role now during permitting processes to develop local 5G infrastructure quickly with minimal security risks. In addition, with the proliferation of artificial intelligence assets, the data we transmit across all our networks, which have historically been unclassified in open domains, has now been weaponized through data analytics. We need not look any further than the ability to use a military member's i-watch and fit-bot location and physical exertion data to determine military unit movements. We are in the process of a complete review of data classifications which drive a huge increase in the need for secure communication networks in special compartmentalized information facilities (SCIFS).

In addition, the rapidly advancing technology to enable smart cities and industries has outrun the security needed to protect our lives, privacy, and resources. Recent intelligence and government warnings have highlighted control system cybersecurity as a critical national vulnerability. Cyber-attacks targeting building systems can result in the takedown of key weapon systems, as well as threatening privacy, safety, and lives of our citizens on our installations, in our homes, in our cars, and in public places. Responding to these challenges, we are dedicating resources to improve our control system resilience starting with inventories, cyber-hygiene, and monitoring. Ultimately control system security will require a national action plan.

Responding to emerging threats to the physical security of our installations is critically important to ensure continuity of our mission while protecting our people. Installations and ranges will need the assistance of defense communities and States to assist with outside-the-fenceline physical protections of threats from unmanned systems, foreign surveillance, encroachment, and access to military bases. Data collected from sensors on our ranges and from seemingly innocuous surveys for other exploratory or natural resource protection purposes can be accessed by adversaries to enhance surveillance and reconnaissance activities. As an example the military has processes in place to ensure energy development off shore and on land will not negatively impact critical DOD training and test ranges. The Administration's plan to develop all energy sources is being carried out with innovative agreement to ensure the long term resilience of ranges to support future weapon system development.

We also face an array of challenges for installations and ranges to be environmentally resilient. We consider the impacts of natural disasters, land subsidence, wildfires, droughts, and incompatible development as issues affecting our ability to train, test, and operate. It is difficult to predict where the next flood, hurricane, tornado, or earthquake will hit, but must continue to invest, innovatively in the modernization and repair of facilities and infrastructure to build resilience, as opposed to abandoning critical capabilities.

These threats require holistic solutions, not focusing on just one issue. We will also require innovation with our defense community partners to develop and successfully modernize our installations. We have taken an important step in this drive for innovation by standing up an Acquisition Modernization Office (AMO) within Naval Facilities Command to consolidate our activities to acquire services and construction through unique asset management authorities provided to us by Congress. We cannot continue to defer critical projects to reduce our mission risk because of limited military construction or facility modernization account funding. We

also have the opportunity to fundamentally change the business practices we use for installation support to integrate with local communities and regions.

We must have the flexibility and creativity in a changing world where threats from great powers and regional conflicts are driving our nation's military strategy**. Our definitions of military value are evolving as technology and threats rapidly evolve.** At the same time, our own fiscal realities and the long list of competing demands are requiring new approaches to free up resources and allow investment back into priorities. At the heart of the solutions and strategies to these complex challenges is innovation. We are embracing innovation and entrepreneurship now to accelerate initiatives to make us stronger.